

MITIGATE DATA LOSS THROUGH POLICY-DRIVEN MOBILITY

INTRODUCTION

Enterprise mobility has entered main stream enabling organizations to enhance productivity index by allowing the use of laptops, mobile phones or tablets to some or all of their staff. The Consumerization of IT trend and Bring-Your-Own-Device (BYOD) initiatives allow end users to work with the devices or applications of their choice; allowing to, create, access and share files from within as well as outside the corporate network.

The new age smart mobile devices are changing the way people collaborate within organizations and outside it; often subscribing to consumer-style file sharing platforms like Dropbox to share data with outside parties and to ensure they have up-to-date files on all their devices, potentially putting enterprise information at risk. Business critical information is beyond corporate firewalls, and is constantly accessed and shared through multiple end user devices. Proliferation of enterprise-connected mobile devices are constantly straining IT security resources; data managers are increasingly having nightmares about data landing at the wrong hands.

BYOD is leading the biggest shift in client computing; many leading research organizations indicate that many more CIOs will cease to provide corporate devices to their employees by 2016. However, enterprise IT is reluctantly embracing BYOD policies that challenge information security, device management and control, and workspace delivery. Unfortunately, security policies, content sharing tools, and device management tools are all inconsistently implemented across multiple platforms. Enterprise IT should collaborate with end users and business managers to proactively create policies that are consistent with organizational programs anticipating future requirements of data mobility.

CHALLENGES OF UNPLANNED MOBILITY

A leading IT research firm in their recent report on Enterprise File Sync and Share (EFSS) market concludes that organizations that are overlaying EFSS solution to existing policies around data protection and information governance should reconsider, since with simplified data accessibility, end users will create more data challenging existing protection policies raising stakes for governance. Data managers will need to keep in mind emerging technologies and the ever growing needs of their end users to devise policies that are futuristic yet supporting the larger interests of data confidentiality and consistency.

Typically, NAS devices and file servers are being used for file sharing within corporate setup, and file protection in remote locations. But with increasingly mobile end users, it is cumbersome for files to be shared or backed up with slower network performance, especially with VPN-constrained access. As a result, files residing in end user endpoints are not protected and shared.



In addition, anywhere access of files is key for remote executives and road warriors. The ability of administrators to control and manage these access rights is key to security and efficiency of the organization. The need of the hour is for the administrators to be able to provide selective access based on geographical location or IP address or time of access; these protocols ensure unauthorized access to business critical information.

INDUSTRY BEST PRACTICES

The starting point for a CIO or IT Manager should be to conduct an audit to determine what their organization have and what the priorities should be. This should include not just the mobile infrastructure, end users, devices and applications, but also the data, its sources, the flow of data and its access to determine the inventory, risks, liabilities and costs.

The next step should be to engage the business units and a subset of end users to understand their requirements and what data mobility means to them to do their job effectively. IT should functionally profile their users to determine user requirements and solutions for specific user groups, work styles and work spaces. Not all users are mobile workers, and in certain cases, users have higher risk than others. Broader policies and standardized technology need not apply to all users. This document should help the stake holder in determining the high level strategies that align with wider business goals of the organization and the places to implement them.

In the past, implementations of enterprise mobility management (EMM) have been focused primarily on mobile device management (MDM) and mobile application management (MAM) areas. This approach and associated technologies focus only on controlling the whole mobile device or a set of mobile applications, which are approved by the organization. To control data in a more granular way, mobile content management (MCM) solutions have started gaining popularity recently. MCM allows organizations to control how data is accessed, shared or changed as it goes on to the mobile devices. To reduce and control the risks associated with your data; consider all the following aspects about it as it flows across your organization from its birth to its logical conclusion:

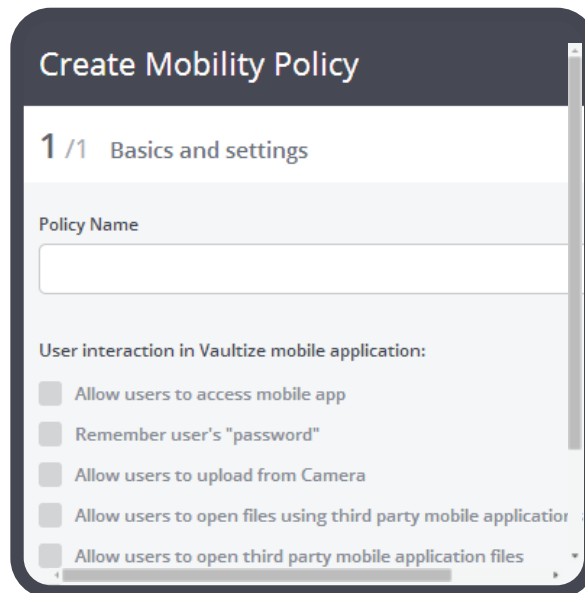
- **End-to-end security:** Ensure that the data is secured right from its source, across its routes, and to the point of deletion through means of encryption-at-source, in transit and at rest, data privacy and data integrity.
- **Data access control:** Determine which data sources can be accessed from anywhere using mobile or even non-mobile devices, determine rights of users on various devices, locations and scenarios, and determine what users can do with the data.
- **Managed data mobility:** Containerize the data on mobile devices so that chances of loss or non-compliance are near zero. MCM is a very important facet of this requirement. Containerization also includes encryption on mobile storage and the ability to securely wipe the container based on policies.
- **Data protection:** Data should always remain encrypted on endpoint storage (mobile or non-mobile), with the ability to wipe it securely from remote location. In addition, data versioning should be possible for better recovery of lost data.
- **Managed sharing and collaboration:** Manage sharing of data inside as well as outside the organization through any of the workflows end users are comfortable with, viz. as attachments in mails, through FTP or through sync.
- **Compliance:** Includes retention and deletion of copies or versions of data, encryption key management, data privacy, location of data, access control, and complying with various internal and external policies or regulations.

CORE POLICIES TO SUPPORT YOUR MOBILITY INITIATIVES

1. Data Mobility Policy

Mobility policy is to govern content usage rights by the end users on their mobile devices. These policies will ensure administrators have comprehensive control over content that are residing in end user devices, and what level of usage are allowed by these users. Policies selectively allow users to perform the below functions, not limiting to:

- Opening files (including opening in third party applications)
- Sharing files (including with whom files can be shared)
- Copying and/or pasting content
- Printing
- Emailing, etc.



2. Data Sharing Policy

Data sharing policy is essential to outline how users can share the data, within corporate network or outside. Typically for someone with access to EFSS client (e.g. an employee), the data is accessible through the client. But for someone with no access to EFSS client and is outside corporate network (e.g. an outside party), a web link (URL) can be provided via an email. Data can be downloaded or only viewed through online viewer depending on the policy specified. If a link is being provided, there should be an option to make it password protected, and in addition, giving expiration time for additional protection. Once this expiration time is passed, the link should automatically be deactivated.

Enterprise IT should investigate a new tool that allow for specific sharing policies that restrict who accesses, what, from where. 'Fencing' is yet another way to apply specific policies for data sharing that is based on either geographic restriction or IP address restriction.

With geo fencing, administrators should be able to choose the list of countries from where access should be restricted. With IP/domain fencing, data sharing is restricted to certain IP addresses, which can be enlisted by the administrator in the management console.

3. Anywhere Access Policy

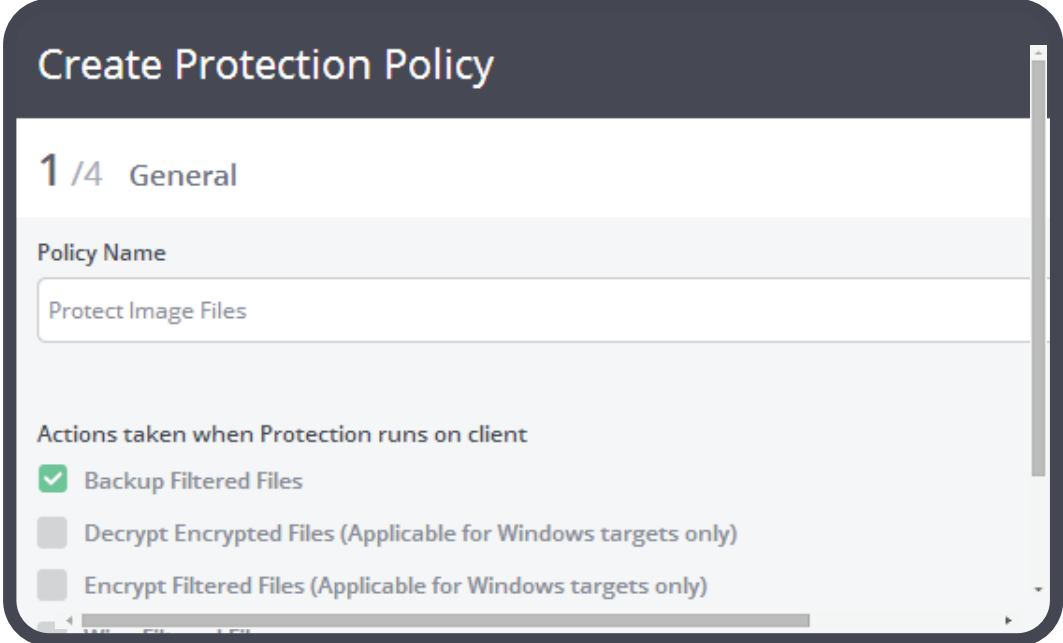
Anywhere Access policy is ideally suited for data access from corporate file servers and NAS to end users when they are outside the corporate network beyond firewall. The changes made by user on the device is synced back to file server to ensure consistency. Through anywhere access policies, the enterprise IT should securely extend the perimeter of their corporate network to include mobile devices beyond firewall - facilitating easy access and sharing for improved productivity.

4. Access Control Policy

Access Control policy should be created by administrator to provide data access to an end user from the endpoints that has the requisite EFSS client. As part of the policy, the user could be permitted to perform multiple actions such as edit the data, upload data, etc.



5. Protection Policy



Create Protection Policy

1 / 4 General

Policy Name

Protect Image Files

Actions taken when Protection runs on client

- Backup Filtered Files
- Decrypt Encrypted Files (Applicable for Windows targets only)
- Encrypt Filtered Files (Applicable for Windows targets only)

Every organization thinks differently when it comes to what data to protect. The IT policies should allow to completely control what data to filter out, and also allow to specify how long to keep the versions of the data. Enterprise IT should choose some of the below policies to manage their file-size quota optimally, and at the same time retain the versions based on the need of the organization:

- Include files or folders for data protection
- Exclude files or folders for data protection
- Exclude files bigger than
- Exclude files smaller than
- Exclude files older than, etc.

6. Schedule and Retention Policies

File sync and sharing tools typically allow you to choose the type of data backup it requires, depending on the business policies. Some of the most common policies are:

- Continuous – allows to continuously monitor the modifications made to the data and sends the incremental changes as soon as those are saved to the disk
- Periodic – allows specifying the periodicity of the data protection. The incremental data protection will be performed every 'N' minutes or every 'N' hours, as specified by the administrator
- Dates of month – allows to schedule the incremental data protection at some fixed time on certain dates of the month
- Days of week – allows to schedule the incremental data protection at some fixed time on certain days of the week
- Stop after – allows to schedule the data protection to stop after some time (in hours and minutes)

7. Network Policy

Network policies allow administrators to define data upload and data backup based on network bandwidth availability and costs.

Bandwidth Details:

Administrators should be able to identify and use optimizations like differential change extraction, de-duplication and compression, utilizing their existing network bandwidth optimally. This way bandwidth usage is automatically controlled.

Mobile Data Limit:

Vaultize allows to limit the data usage for mobile on per month basis. In addition, policies should enable administrators to allow access based on the type of mobile data access, for example, end users can be given the option to access files or folders only through the corporate Wi-Fi, and alerted when end users switch over to different network or to packet data.

VAULTIZE'S POLICY-DRIVEN APPROACH FOR RISK AVERSION

Vaultize offers enterprise platform that enables MCM, mobile data containerization, file sharing and sync, secure anywhere access to corporate data repositories with end-to-end security and data loss protection.

Vaultize is at the fore front of cutting edge innovation that allows corporates to create and enforce policies to fearlessly allow end users to create, access, share critical information via any mobile device of choice. Vaultize enables administrators to get complete control over the policies in order to effectively customize data protection, data access and data sharing according to your organization's requirements.

ABOUT VAULTIZE

Vaultize enables enterprises to embrace file sharing & data mobility for improved collaboration and productivity yet not compromise on data security or IT control. Vaultize offers end-to-end protection through a highly secure mobility platform that provides endpoint backup and encryption, and file sync/share. Vaultize differentiates through military-grade data encryption, deduplication and compression at source, data privacy options, remote data visibility & control, and the ability to deploy either through public cloud or private cloud.

For more information, visit www.vaultize.com